Prof. Dr. Andreas Podelski
Dominik Klumpp
Frank Schüssele

Hand in until January 27th, 2021
23:59 via ILIAS
Discussion: February 1st/2nd, 2021

# Tutorial for Cyber-Physical Systems - Discrete Models

## Exercise Sheet 10

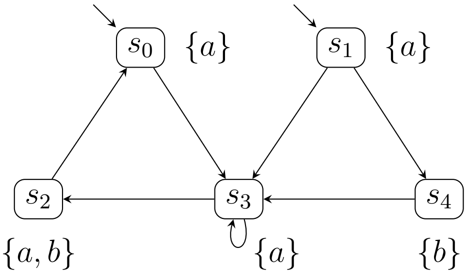
**Exercise 1$^\star$: Evaluation** 1 Bonus Point

Complete the lecture evaluation

**Exercise 2: Invariant checking I** 4 Points

In the lecture, you have seen an algorithm for invariant checking by forward depth-first search. This algorithm is displayed in algorithm 1.

Apply this algorithm to the following transition system whose set of atomic propositions is $AP = \{a, b\}$. The invariant $\Phi$ to be checked is the propositional logical formula $a$.



Whenever you iterate over a set of states, always take state $s_i$ before state $s_j$ if $i$ is smaller than $j$.

Present the execution of the algorithm by writing down the contents of the set $U$ and the stack $\pi$ directly before every call to the function **DFS**.

**Exercise 3$^\star$: Invariant checking II** 2 Bonus Points

The "DFS-based invariant checking" algorithm presented in algorithm 1 (and in the lecture) always computes a minimal counterexample (minimal in the sense that you cannot remove the last state). However, the algorithm does not necessarily compute a counterexample of minimal length (there might be two minimal counterexamples of different lengths). What is an example that shows that the counterexample that is returned does not always have minimal length? For this purpose, provide the following:

- A transition system that has three states $s_0, s_1, s_2$.
- An invariant.
- The counterexample with non-minimal length that is computed by the algorithm that uses the following strategy for iterating over a set of states: always take state $s_i$ before state $s_j$ if $i$ is smaller than $j$.
- A counterexample of minimal length.

**Algorithm 1:** DFS-based invariant checking

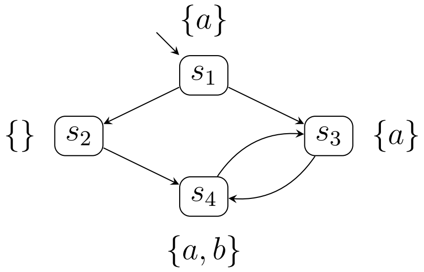
```
input  : a finite transition system $\mathcal{T}$ and a propositional formula $\Phi$
output: "yes" if $\mathcal{T} \models$ "always $\Phi$", otherwise "no" and a counterexample
$U := \emptyset$;                                           // set of states
$\pi := \varepsilon$;                                       // stack of states
forall $s \in I$ do
    if DFS($s, \Phi$) then
        return("no", $reverse(\pi)$);                       // path from $s$ to error state
    end
end
return("yes");                                              // $\mathcal{T} \models$ ``always $\Phi$''

function DFS($s, \Phi$)
    $push(s, \pi)$;
    if $s \notin U$ then
        $U := U \cup \{s\}$;                                // mark $s$ as reachable
        if $s \not\models \Phi$ then
            return("true");                                 // $s$ is an error state
        else
            forall $s' \in Post(s)$ do
                if DFS($s', \Phi$) then
                    return("true");                         // $s'$ lies on a path to an error state
                end
            end
        end
    end
    $pop(\pi)$;
    return("false");
end
```

**Exercise 4: Paths and Traces** 6 Points

*The following exercise should help you to understand the differences between paths and traces and the corresponding fragments.*

Consider the following transition system with the set of atomic propositions $AP = \{a, b\}$.



Solve the following tasks.

(a) Give examples that illustrate the difference between the different notions of paths and path fragments. Therefore give the following path fragments of the given transition system:

- A path fragment that is neither initial nor maximal
- An initial path fragment that is not maximal
- A maximal path fragment that is not initial
- An initial and maximal path fragment (i.e. a path)

(b) Reformulate task (a), but now for traces instead of paths and then solve the task.

(c) Give an example of a non-maximal path fragment that is not a path fragment of the transition system.

(d) Give an example of a non-maximal trace fragment that is not a trace fragment of the transition system.

(e) Give an example of a path that is not a path of the transition system.

(f) Give an example of a trace that is not a trace of the transition system.

**Exercise 5: Complement of LT-Properties** 4 Points

*This exercise is supposed to reveal some interesting (and possibly counter-intuitive) facts about LT properties and their complement.*

Determine if the following statements hold for every trace $\tau \in (2^{AP})^\omega$, transition system $T$ over $AP$ and property $E \subseteq (2^{AP})^\omega$.

If a statement holds, give a proof. Otherwise give a counterexample.

(a) If $\tau \models \neg E$ holds, does it follow that $\tau \not\models E$ holds?

(b) If $\tau \not\models E$ holds, does it follow that $\tau \models \neg E$ holds?

(c) If $T \models \neg E$ holds, does it follow that $T \not\models E$ holds?

(d) If $T \not\models E$ holds, does it follow that $T \models \neg E$ holds?

**Notes:**

- The negation of a property $E$ is defined as $\neg E := (2^{AP})^{\omega} \setminus E$
- A trace $\tau$ satisfies a property $E$, $\tau \models E$ if and only if $\tau \in E$